UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/055,407	01/23/2002	David A. Fertell	3361-011773	7264

7590 07/02/2008

Webb Ziesenheim Logsdon Orkin & Hanson, P.C.
Suite 700
436 Seventh Avenue
Pittsburgh, PA 15219

EXAMINER	
DENNISON, JERRY B	
ART UNIT	PAPER NUMBER
2143	
MAIL DATE	DELIVERY MODE
07/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/055,407
Filing Date: January 23, 2002
Appellant(s): FERTELL ET AL.

William H. Logsdon
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 22 April 2008 appealing from the Office action mailed 20 June 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,113,994	Swift et al.	9-2006
2006/0077977	Caronni et al.	4-2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 22-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Swift et al. (U.S. 7,113,994).

1. Regarding claim 22, Swift disclosed a system and method of proxy authentication in a secured network, in which a user first registers, with a trusted security server proxy, authorization information and identifies the proxy client and specifies the extent of proxy authority granted to the proxy client (Swift, col. 2, lines 30-35) and if the security server verifies that the request is within the proxy authority granted to the proxy client, the security server returns to the proxy client a data structure containing information recognizable by the target service to authenticate the proxy client for accessing the target service on behalf of the user (Swift, col. 2, lines 38-43). As shown in Fig. 2, the

proxy client 74 uses the proxy authentication data 92, provided by the Trusted security server 80, to access and use the target service 76.

Therefore, Swift disclosed a method of controlling computer network access comprising:

(a) initiating a communication session between a first computer and a second computer (Swift, Fig. 2, 84, proxy permission request);

(b) receiving at the first computer from the second computer via the communication session an access configuration including a control setting for at least one communication protocol (Swift, Fig. 2, 90, proxy client receives proxy authentication data to access the target service);

(c) monitoring data conveyed to or from a process running on the first computer based on the control setting (col. 5, lines 40-55, target service uses the authentication data for authenticating the proxy client when the proxy client attempts to access the target service); and

(d) controlling the data conveyed to or from the process based on the control setting (col. 5, lines 40-55, target service uses the authentication data for authenticating the proxy client when the proxy client accesses and uses the target service).

2. Regarding claim 23, Swift disclosed the limitations, substantially as claimed, as described in claim 22, including wherein the process instantiates another communication session; and the conveyance of data is controlled in connection with the other communication session (col. 5, lines 40-55, target service uses the authentication

data for authenticating the proxy client when the proxy client attempts to access the target service).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-9, 13-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Swift et al (U.S. 7,113,994) in view of Caronni et al (U.S. 2006/0077977).

3. Regarding claims 1 and 13, Swift disclosed a system and method of proxy authentication in a secured network, in which a user first registers with a trusted security server proxy authorization information and identifies the proxy client and specifies the extent of proxy authority granted to the proxy client (Swift, col. 2, lines 30-35) and if the security server verifies that the request is within the proxy authority granted to the proxy client, the security server returns to the proxy client a data structure containing information recognizable by the target service to authenticate the proxy client for accessing the target service on behalf of the user (Swift, col. 2, lines 38-43). As shown in Fig. 2, the proxy client 74 uses the proxy authentication data 92, provided Trusted security server 80, to access and use the target service 76.

Therefore, Swift disclosed a method for controlling computer network access, the method comprising the steps of:

(c) initiating at the client computer a second communication session at the second network address (Swift, Fig. 2, 84, proxy permission request);

(d) receiving at the client computer via the second communication session an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session (Swift, Fig. 2, 90, proxy client receives proxy authentication data to access the target service);

(e) instantiating on the client computer a process which initiates a third communication session at a third network address (Swift, Fig. 2, 92, proxy client sends connection request to target service using the proxy authentication data); and

(f) in connection with the third communication session, controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the control setting for the one communication protocol (col. 5, lines 40-55, target service uses the authentication data for authenticating the proxy client when the proxy client accesses and uses the target service).

Swift disclosed the internet client to initiate communication with the trusted secure server (Fig. 2, 84). In order for this to occur, the proxy device must be aware of the trusted security server's address.

However, Swift did not explicitly state how the proxy client obtained the address of the trusted security server, or in other words, did not explicitly state how the proxy client became aware of the trusted security server's presence on the network.

This would have motivated one of ordinary skill to search the prior art for well-known techniques for discovering devices or obtaining addresses of devices on the network.

In an analogous art of networking, Caronni disclosed a system and method where a web client 1102 obtains an address to a web server1104 from computer system 1106 (Caronni, Fig. 11, [0079]).

Caronni provides a method for obtaining an address of a device by obtaining the address from computer system whose address is already known by the Internet client. As such, Caronni provides teaching that includes a technique for finding the address of a device.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made for the internet client of Swift to use the teachings of Caronni in order to obtain an address of a secure server before initial communication with the secure server in order to learn of the secure server's existence and to be able to use the services of the secure server.

Claim 13 includes limitations that are substantially similar to claim 1. Therefore claim 13 is rejected under the same rationale.

4. Regarding claims 2 and 19, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claims 1 and 13, including wherein:

the access configuration includes a list related to the control setting for the one communication protocol and the conveyance of data via the third communication

session is controlled based on the list (Swift, col. 5, lines 14-20, the authorization data may specify which services the proxy client is allowed to access on the user's behalf; lines 45-50, the data structure may be in the form of capabilities).

5. Regarding claim 3, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claim 1. Swift also provided examples of services to include secure file access (Swift, col. 1, lines 25-30).

Swift did not provide a specific type of secure file access [i.e. World Wide Web (Web); file transfer protocol (FTP); E-mail; News; Chat; Instant Messaging; Telnet; and Peer-to-Peer].

This would have motivated one of ordinary skill in the art to search the prior art for standard types of secure file access. It was well known in the art at the time the invention was made that protocols such as World Wide Web and file transfer protocol include secure file access.

Examiner takes Official Notice (see MPEP § 2144.03) that World Wide Web and file transfer protocol were well known types of secure file access in the art at the time the invention was made. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to use the World Wide Web and file transfer protocol as the protocol in Swift for the benefit of using a standard protocol that is already used by the public without having to reinvent the wheel.

The Applicant is entitled to traverse any/all official notice taken in this action according to MPEP § 2144.03, namely, "if applicant traverses such an assertion, the

examiner should cite a reference in support of his or her position". However, MPEP § 2144.03 further states "See also *In re Boon*, 439 F.2d 724, 169 USPQ 231 (CCPA 1971) (a challenge to the taking of judicial notice must contain adequate information or argument to create on its face a reasonable doubt regarding the circumstances justifying the judicial notice)." Specifically, *In re Boon*, 169 USPQ 231, 234 states "as we held in *Ahlert*, an applicant must be given the opportunity to challenge either the correctness of the fact asserted or the notoriety or repute of the reference cited in support of the assertion. We did not mean to imply by this statement that a bald challenge, with nothing more, would be all that was needed". Further note that 37 CFR § 1.671(c)(3) states "Judicial notice means official notice". Thus, a traversal by the Applicant that is merely "a bald challenge, with nothing more" will be given very little weight.

6. Regarding claim 4, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claim 1, including wherein the control setting is one of:

unrestricted computer network access (Allow All);

no computer network access (Block All);

limited computer network access to network addresses included in an allow list (Allow Listed); and

unrestricted computer network access except to network addresses included in a block list (Block Listed) (Swift, col. 5, lines 14-20, the authorization data may specify

which services the proxy client is allowed to access on the user's behalf; lines 45-50, the data structure may be in the form of capabilities).

7. Regarding claims 5 and 16, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claims 1 and 13, including wherein:

the access configuration further includes at least one of the following global control settings:

access prohibited to conveyed data including a predetermined word or phrase;

access prohibited to data of at least one predetermined data type;

access prohibited to data conveyed during at least one of a predetermined time and day-of-week; and

access prohibited based on a rating for a category included with the conveyed data; and step (f) further includes the step of controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the at least one global control setting (Swift, col. 8, line 16).

8. Regarding claim 6, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claim 5. Swift and Caronni did not explicitly state wherein the at least one predetermined data type includes an Internet cookie.

Examiner takes Official Notice (see MPEP § 2144.03) that using cookies to determine access permissions for clients in a network was well known in the art at the time the invention was made.

9. Regarding claims 7 and 15, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claims 1 and 13. Swift and Caronni did not explicitly state further including at least one of: after step (b), the step of terminating the first communication session; and after step (d), the step of terminating the second communication session.

However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to end these sessions since the requested data was provided (i.e. the computer system of Caronni provides an address, and the secure server of Swift provides the authorization data).

Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to end the sessions since the requested data was provided and there is no longer any need to continue communication with these devices, for the benefit of freeing up communication ports for reuse.

10. Regarding claims 8 and 18, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claims 1 and 13. Swift and Caronni did not explicitly state transmitting from the client computer via the second communication session a request to receive another access configuration including a control setting for the one communication protocol;

receiving at the client computer via the second communication session the other access configuration;

and performing step (f) based on the control setting included in the other access configuration.

However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to repeat the steps in Swift and Caronni in order to obtain authorization for other target services.

11. Regarding claims 9 and 21, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claims 1 and 13. Swift and Caronni did not explicitly state wherein step (f) further includes the steps of: determining from the conveyed data the communication protocol thereof, and determining from the thus determined communication protocol the control setting therefor. However, it would have been obvious to one of ordinary skill in the art that when a communication is received and understood, the protocol must be determined, otherwise, the communication would fail. It would have also been obvious that the target service must determine the access permissions of the proxy client, otherwise there would be no reason for the proxy client to retrieve these permissions in the first place.

12. Regarding claim 14, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claim 13, including wherein the first and second server computers are the same server computer (Swift, Fig. 2, 80).

13. Regarding claim 17, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claim 16, including wherein: prior to receipt of the access configuration at the client computer, the control setting for the one communication protocol is selected from a plurality of different control settings therefor;

and each global control setting is selected nonexclusively of any other global control settings (Swift, col. 5, lines 40-55).

14. Regarding claim 20, Swift and Caronni disclosed the limitations, substantially as claimed, as described in claim 19, including wherein the entry comprises a network address (Swift, col. 5, lines 15-20, proxy auth data identifies one or more clients).

(10) Response to Argument

Claims 1 and 13

Regarding claims 1 and 13 under 35 U.S.C. 103(a), Appellants present three principal arguments:

a) That "equating proxy client 74 in the Swift et al. document with the client computer in claim 1 is improper" (Br. 6, ¶ 1).

b) That "the Swift et al document discloses, teaches and suggests controlling access and, hence, the conveyance of data, at a completely different location than the control of conveyance of data in claim 1 which is controlled by the control setting received at the client computer" (Br. 6, ¶ 2).

c) That the Examiner has not provided sufficient motivation to combine or modify the cited references and "the teachings of the Caronni et al. document are not logically combinable with the teachings of the Swift et al. document (Br. 6-8).

d) That "there is no disclosure, teaching or suggestion in the Swift et al. and Caronni et al. documents, either individually or in combination, to provide a first communication session between a client computer and a first server computer and to initiate a second communication session between the client computer and a second server computer as claimed in claim 13" (Br. 9).

Regarding argument a) that "equating proxy client 74 in the Swift et al. document with the client computer in claim 1 is improper" (Br. 6, ¶ 1), Examiner respectfully disagrees. Applicant attempts to show why this is improper by showing a distinction between user 70 and proxy client 74 (Br. 6, ¶ 1).

Examiner notes that claim 1 does not recite any type of distinction between a user and a device, does not require a user to be at any specific device, and does not even recite a user for the matter. As such, Applicant's remarks regarding distinguishing between user and proxy client are irrelevant.

Applicant does not provide any arguments regarding whether the proxy client of Swift performs the functionality of the claimed client computer.

As shown in the above rejection of claim 1, the proxy client of Swift was relied upon to disclose:

(c) initiating at the client computer a second communication session at the second network address (Swift, Fig. 2, 84, proxy permission request);

(d) receiving at the client computer via the second communication session an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session (Swift, Fig. 2, 90, proxy client receives proxy authentication data to access the target service);

(e) instantiating on the client computer a process which initiates a third communication session at a third network address (Swift, Fig. 2, 92, proxy client sends connection request to target service using the proxy authentication data); and

(f) in connection with the third communication session, controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the control setting for the one communication protocol (col. 5, lines 40-55, target service uses the authentication data for authenticating the proxy client when the proxy client accesses and uses the target service).

As shown above, the proxy client (c) initiates a communication session with a second computer by sending a "proxy permission request", and then (d) receives an access configuration including a control setting for a protocol by receiving proxy authentication data to access the target service. The Swift reference disclosed "If the trusted security server 80 determines that the proxy client 74 should be permitted to access the target service 76 on behalf of the user 70, it creates a data structure 90 containing authentication information recognizable by the target service 76 for authenticating the proxy client acting as the user to access the target service. The format and contents of the proxy authentication data structure 90 depends on the security protocols used and their implementations in the network system" (See Swift, col. 5, lines 35-43). Swift further disclosed that the proxy authentication data structure is given to the proxy client, and the proxy client includes this data structure in an access request to the target service (Swift, col. 5, lines 47-53). The proxy client then (e) instantiates a process that initiates a third session at a third address, by sending a connection request to target service using the proxy authentication data, and (f) control

the conveyance of data to or from the proxy client using the control setting for the protocol by sending the authentication data for authenticating the proxy client when the proxy client accesses and uses the target service. Every time the proxy client accesses the target service, it must provide the proper secret key, (further explained in col. 6, lines 4-25, and 38-46 "after accepting the user's password and deriving the user's long-term key, the Kerberos client 100 on the user's computer sends a request 112 to the KDC 106 for a session key and a session ticket for use in subsequent transactions with the KDC during this logon session). Without the use of the session key and session ticket, communication would not occur as the proxy client would not be providing the proper credentials. In order for the conveyance of data to occur properly, the proxy client must provide the data in the proper format which requires the credentials.

Therefore, from the rejection above, it is shown that the proxy client computer performs the functions of the claimed client computer. Therefore, it is reasonable to interpret the proxy client computer as the claimed client computer. Common sense also shows that a "proxy client" computer clearly acts as a client computer, as the name itself suggests. As such, equating the proxy client in the Swift reference with the client computer of claim 1 is proper. As such, it is believed that the rejection should be maintained.

Regarding argument b) that "the Swift et al document discloses, teaches and suggests controlling access and, hence, the conveyance of data, at a completely different location than the control of conveyance of data in claim 1 which is controlled by

the control setting received at the client computer" (Br. 6, ¶ 2), Examiner respectfully disagrees.

Claim 1 recites in section (f), "controlling the conveyance of data...based on the control setting for the one communication protocol." This control setting was provided to the client in section (d) of the claim. Therefore, while the client is controlling the conveyance of data, such control was provided to the client.

The Swift reference disclosed "If the trusted security server 80 determines that the proxy client 74 should be permitted to access the target service 76 on behalf of the user 70, it creates a data structure 90 containing authentication information recognizable by the target service 76 for authenticating the proxy client acting as the user to access the target service. The format and contents of the proxy authentication data structure 90 depends on the security protocols used and their implementations in the network system" (See Swift, col. 5, lines 35-43). Swift further disclosed that the proxy authentication data structure is given to the proxy client, and the proxy client includes this data structure in an access request to the target service (Swift, col. 5, lines 47-53). The proxy client controls the conveyance of data between the proxy client and the target service by sending the authentication data for authenticating the proxy client when the proxy client accesses and uses the target service. Every time the proxy client accesses the target service, it must provide the proper secret key, (further explained in col. 6, lines 4-25, and 38-46 "after accepting the user's password and deriving the user's long-term key, the Kerberos client 100 on the user's computer sends a request 112 to the KDC 106 for a session key and a session ticket for use in subsequent

transactions with the KDC during this logon session). Without the use of the session key and session ticket, communication would not occur as the proxy client would not be providing the proper credentials. In order for the conveyance of data to occur properly, the proxy client must provide the data in the proper format which requires the credentials.

Therefore, just as claims 1 and 13 require, the control setting was provided to the client and used by the client to control the conveyance of data to the target service. Without the data structure, session key, and session ticket (which provide settings in accordance with a security protocol), the conveyance of data would not be authorized and communication would not properly occur. As such, it is believed that the rejection should be maintained.

Regarding argument c) that the Examiner has not provided sufficient motivation to combine or modify the cited references and "the teachings of the Caronni et al. document are not logically combinable with the teachings of the Swift et al. document (Br. 6-8), Examiner respectfully disagrees.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re*

Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, motivation was found in the knowledge generally available to one of ordinary skill in the art.

Swift disclosed a method for controlling computer network access as shown in the rejection. In order for the system of Swift to properly function, the proxy device must be aware of the trusted security server's address. However, Swift did not explicitly state how the proxy client obtained the address of the trusted security server, or in other words, did not explicitly state how the proxy client became aware of the trusted security server's presence on the network. This would have motivated a network administrator to find a well known way for discovering devices in order to allow for the system of Swift to properly function when the address of the server is not known by the proxy client. Caronni disclosed a well known way of obtaining an address of a device by obtaining the address from a computer system whose address is already known by the proxy client. Since Swift remains silent on how the proxy client obtained the address of the trusted security server, one of ordinary skill in the art would have recognized that the teachings of Caronni could be used to provide the appropriate device discovery method. Doing so would have been nothing more than combining familiar elements according to known methods, to achieve the predictable result of obtaining an address of a device before initial communication with the device in order to learn of the secure server's existence and to be able to use the services of the device. This motivation to combine the references meets the KSR exemplary rationale (See MPEP 2143) of at least: (A)Combining prior art elements according to known methods to yield predictable results; (D)Applying a known technique to a known device (method, or product) ready

for improvement to yield predictable results; (E)"Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; (F)Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art.

In response to Applicant's argument that "the teachings of the Caronni et al. document are not logically combinable with the teachings of the Swift et al. document" (Br. 6-8), Examiner respectfully disagrees. One of ordinary skill in the art would have been motivated to combine their teachings since both teachings provide for submitting a request for data over an IP network (Caronni, [0023]; Swift, col. 4, lines 30-37), and modifying the proxy client to simply submit another type of request does not involve any extensive implementation. As such, it is believed that the rejection should be maintained.

Regarding argument d) that "there is no disclosure, teaching or suggestion in the Swift et al. and Caronni et al. documents, either individually or in combination, to provide a first communication session between a client computer and a first server computer and to initiate a second communication session between the client computer and a second server computer as claimed in claim 13" (Br. 9), Examiner respectfully disagrees. As shown in the rejection, Swift was relied upon for initiating a second communication session with a second server to retrieve the access configuration data. Caronni was relied upon for accessing a known computer to obtain the address of an

unknown computer. Therefore, it is the combination of the references that disclosed the invention as claimed in claim 13.

Applicant states that "This is admitted by the Examiner in the rejection of claim 14, wherein the Examiner states that "the first and second server computers are the same server computer (Swift et al, Fig. 2, 80)" (Br. 9).

It appears Applicant is in agreement that the reference(s) disclosed the limitation of claim 14, as Applicant did not provide any arguments against the mapping. Examiner notes that the rejection of claim 14 does not provide any type of admission that the reference(s) do not disclose the limitations of claim 13. As such, it is believed that the rejection should be maintained.

Claims 8 and 18

Regarding claims 8 and 18 under 35 U.S.C. 103(a), Appellants present three principal arguments:

a) That there is "no disclosure, teaching or suggestion in the Swift et al. and Caronni et al documents, either individually or in combination, to provide another access configuration." And that the "rejection of claims 8 and 18 is based on hindsight"

Regarding argument a) that there is "no disclosure, teaching or suggestion in the Swift et al. and Caronni et al documents, either individually or in combination, to provide another access configuration." And that the "rejection of claims 8 and 18 is based on hindsight", Examiner respectfully disagrees.

Dependent claims 8 and 18 simply repeat the limitations of claims 1 and 13 with another access configuration. As explained in the rejection, it would have been obvious to one of ordinary skill in the art at the time the invention was made to repeat the steps of claims 1 and 13 in order to obtain authorization for other target services. The mere function of repeating the steps does not provide reason for patentability, especially when the outcome is the same, in this case, using a control setting in an access configuration to access a service.

Claims 22 and 23

Regarding claim 22, Applicant reiterates the same arguments provided in **argument b)** under claims 1 and 13.

As explained above, The Swift reference disclosed "If the trusted security server 80 determines that the proxy client 74 should be permitted to access the target service 76 on behalf of the user 70, it creates a data structure 90 containing authentication information recognizable by the target service 76 for authenticating the proxy client acting as the user to access the target service. The format and contents of the proxy authentication data structure 90 depends on the security protocols used and their implementations in the network system" (See Swift, col. 5, lines 35-43). Swift further disclosed that the proxy authentication data structure is given to the proxy client, and the proxy client includes this data structure in an access request to the target service (Swift, col. 5, lines 47-53). The proxy client controls the conveyance of data between

the proxy client and the target service by sending the authentication data for authenticating the proxy client when the proxy client accesses and uses the target service. Every time the proxy client accesses the target service, it must provide the proper secret key, (further explained in col. 6, lines 4-25, and 38-46 "after accepting the user's password and deriving the user's long-term key, the Kerberos client 100 on the user's computer sends a request 112 to the KDC 106 for a session key and a session ticket for use in subsequent transactions with the KDC during this logon session). Without the use of the session key and session ticket, communication would not occur as the proxy client would not be providing the proper credentials. In order for the conveyance of data to occur properly, the proxy client must provide the data in the proper format which requires the credentials.

Therefore, just as claims 1 and 13 require, the control setting was provided to the client and used by the client to control the conveyance of data to the target service. Without the data structure, session key, and session ticket (which provide settings in accordance with a security protocol), the conveyance of data would not be authorized and communication would not properly occur. As such, it is believed that the rejection should be maintained.

In summary, each of the cited references relate to network communication generally. Each limitation of the rejected claims is taught or suggested by the combination of Swift and Caronni and the claims amount to nothing more than the predictable use of prior art elements according to their established functions. For at least these reasons, the rejections of claims 1-23 under 35 U.S.C. 103(a) is believed to be proper.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/J. D./

Examiner, Art Unit 2143

Conferees:

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2154

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2151